Lecture 4: Measurements in quantum computing

Rajat Mittal

IIT Kanpur

This lecture will define measurements in the quantum world, i.e., how do we get an output from a quantum system? As before, we need to learn a bit of linear algebra first.

1 Positive semidefinite matrices

Remember that a matrix M is normal if $MM^* = M^*M$. By spectral theorem, these are equivalent to matrices which have an orthonormal basis of eigenvectors. There was no restriction on the kind of eigenvalues for a normal matrix (they could have been any complex number). We got Hermitian matrix (when eigenvalues are real) and unitary matrix (eigenvalues have absolute value 1), when eigenvalues were restricted.

Exercise 1. Prove that a normal matrix is unitary if and only if all eigenvalues have absolute value 1.

A further restriction on eigenvalues of a Hermitian matrix gives us a *positive semidefinite matrix*. A matrix M is positive semidefinite if it is Hermitian and all its eigenvalues are non-negative. If all eigenvalues are strictly positive then it is called a positive definite matrix.

Exercise 2. Show that the matrix $|0\rangle\langle 0|$ is a positive semidefinite matrix. What are its eigenvalues?

We give multiple characterizations of a positive semidefinite matrix.

Theorem 1. *For a Hermitian $n \times n$ matrix $M \in L(V)$, following are equivalent.*

1. $\langle v|M|v\rangle \geq 0$ *for all* $|v\rangle \in V$.
2. *All eigenvalues of M are non-negative.*
3. *There exists a matrix B, s.t., $B^*B = M$ (matrix B need not be square).*

Proof. **1** $\Rightarrow$ **2** : Say, λ is an eigenvalue of M. Then, there exists an eigenvector $|v\rangle \in V$, s.t., $M|v\rangle = \lambda|v\rangle$. So,

$$0 \leq \langle v|M|v\rangle = \lambda\langle v|v\rangle.$$

Since $\langle v|v\rangle$ is positive for all $|v\rangle$, implies the eigenvalue λ is non-negative.
2 $\Rightarrow$ **3** : Since the matrix M is Hermitian, it has a spectral decomposition.

$$M = \sum_i \lambda_i |x_i\rangle\langle x_i|$$

Define $|y_i\rangle = \sqrt{\lambda_i}|x_i\rangle$. Then,

$$M = \sum_i |y_i\rangle\langle y_i|.$$

Exercise 3. What is the problem with λ_i being negative, we have allowed complex numbers?

Define B^* to be the matrix whose columns are y_i. Then it is clear that $B^*B = M$. From this construction, B's columns are orthogonal.

Note 1. In general, any matrix of the form B^*B is positive semi-definite. The matrix B need not have orthogonal columns (it can even be rectangular).

Though, there can be multiple matrices $M_1, M_2 \cdots$ such that $M_1^*M_1 = M_2^*M_2 = \cdots$ (give an example).

This decomposition is unique if B is positive semidefinite. The positive semidefinite B, s.t., $B^*B = M$, is called the square root of M.

Exercise 4. Prove that the square root of a matrix is unique.

Hint: Use the spectral decomposition to find one of the square root. Suppose A is any square root of M. Then use the spectral decomposition of A and show the square root is unique (remember the decomposition to eigenspaces is unique) .

3 $\Rightarrow$ **1** : We are given a matrix B, s.t., $B^*B = M$. Then,

$$\langle v|M|v\rangle = \langle Bv|Bv\rangle \geq 0.$$

Exercise 5. Prove $2 \Rightarrow 1$ directly.

□

Note 2. A matrix M of the form $M = \sum_i |x_i\rangle\langle x_i|$ is positive semidefinite, even if x_i's are not orthogonal to each other (prove it).

Note 3. A matrix of the form $|y\rangle\langle x|$ is a rank one matrix. It is rank one because all columns are scalar multiples of $|y\rangle$. Similarly, all rank one matrices can be expressed in this form.

The following figure (Fig. 1) shows how these special classes are related to each other.

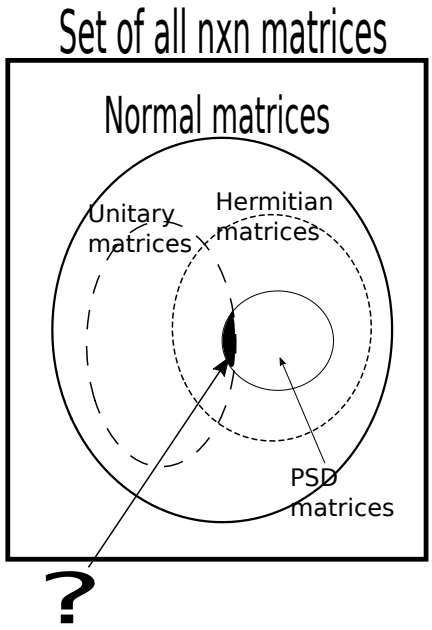


Fig. 1. World of normal matrices

Exercise 6. Identify the area marked with "?" in Fig. 1.

1.1 Projectors

A subclass of interest, of positive semidefinite matrices is called *projectors*. A normal matrix P is called a projector if and only if $P^2 = P$.

Exercise 7. Show that matrix $|0\rangle\langle 0|$ is a projector.

Like the classes seen before, it is not difficult to give a characterization of projectors in terms of their eigenvalues. Suppose, the spectral decomposition of P gives

$$P = \sum_i \lambda_i |x_i\rangle\langle x_i|.$$

We know that $|x_i\rangle$'s form an orthonormal basis. Calculating the square,

$$P = \sum_i \lambda_i^2 |x_i\rangle\langle x_i|.$$

Since spectral decomposition of P^2 is unique and $P^2 = P$, we get that $\lambda_i^2 = \lambda_i$. So, any eigenvalue of a projector is either 0 or 1. In the assignment you will show that if all eigenvalues of a matrix are either 0 or 1, then it is a projector. We get the alternate characterization:

Theorem 2. *A normal matrix P is a projector if and only if all its eigenvalues belong to the set $\{0, 1\}$.*

From spectral decomposition, you can observe that any projector P can be written as $P = \sum_{i=1}^{k} |x_i\rangle\langle x_i|$, where x_i's are orthonormal (though need not form a complete basis). You can extend these set of vectors to get a basis $\{|x_1\rangle, |x_2\rangle, \cdots, |x_k\rangle, |y_{k+1}\rangle, \cdots, |y_n\rangle\}$. Any vector in $\mathbb{C}^n$ can be written as a linear combination of this basis.

$$|\psi\rangle = \sum_{i=1}^{k} \alpha_i |x_i\rangle + \sum_{i=k+1}^{n} \beta_i |y_i\rangle.$$

Applying projector P on vector $|\psi\rangle$, we get,

$$P|\psi\rangle = \sum_{i=1}^{k} \alpha_i |x_i\rangle.$$

In other words, projector P keeps the part on x_i's as it is and zeroes out the part on y_i's. It *projects* on to the subspace spanned by x_i's, and hence it is called a projector. This gives another characterization of an $n \times n$ projector in one to one correspondence with a subspace of $\mathbb{C}^n$. A projector for a subspace S is a matrix which acts as identity on all vectors inside S, and zeroes out anything that is orthogonal to S. Since a projector is a linear operator, this specifies its action on the complete space.

Exercise 8. Given any orthonormal basis $\{x_1, x_2, \cdots, x_k\}$ of a subspace S, show that the projector on S is,

$$P_S = \sum_{i=1}^{k} |x_i\rangle\langle x_i|.$$

Exercise 9. Let P be a projector, show that $I - P$ is also a projector.

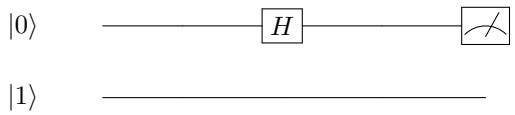
2 Measurement of the system

We have talked about the state of the system and how it evolves. To be able to compute, we should be able to observe/measure the properties of this system too. It turns out that measurement is an integral part of quantum mechanics. Not only does it allow us to determine properties of the quantum system, but it significantly alters the system too.

Before we discuss the third postulate describing the measurements, try to recall if we have seen any measurement before?

With high probability you might have seen it. It is mentioned in many places that if the state is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then it will give $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. That basically meant, if we measure the state in the standard basis $\{|0\rangle, |1\rangle\}$, then the output will be 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.

The following diagram shows how we represent measurement in a quantum circuit. In this case we measure the first qubit but not the second qubit.



Exercise 10. What should be the output of the measurement on the first qubit?

What happens to the state $|\psi\rangle$ itself? It turns out that the final state will be $|0\rangle$ if the output is 0, and $|1\rangle$ if the output is 1. It is as though the state $|\psi\rangle$ is projected onto the space spanned by $|0\rangle$ or $|1\rangle$.

Note 4. If the state remained $|\psi\rangle$ after measurement, we could have performed this measurement multiple times. The statistics obtained would have given us idea about $|\alpha|$ and $|\beta|$. As we mentioned before, this can't be done with just one copy of $|\psi\rangle$. We will see later that a quantum state cannot be copied (no-cloning theorem)

The fact that state gets projected into a basis state, provides the intuition behind the definition of projective measurements. It is a subclass of general measurements we will define later. We would like to say, any partition of the vector space (where the state lives) can be a possible measurement.

Let $|\psi\rangle \in \mathbb{C}^n$ be a state and suppose $P_1, P_2, \cdots, P_k$ are some projectors on orthogonal subspaces which span the space $\mathbb{C}^n$. A measurement on $|\psi\rangle$ using these projections will give state $\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$ with probability $\|P_i|\psi\rangle\|^2$. We divide by $\|P_i|\psi\rangle\|$ so that the resulting state is a unit vector.

Exercise 11. Check that this definition matches with one qubit projection in the standard basis defined above.

Projective measurements: More formally, a projective measurement is described by a Hermitian operator,

$$M = \sum_i m_i P_i, \quad \sum_i P_i = I.$$

Here, P_i's are projectors; for all i, P_i is normal and $P_i^2 = P_i$. If we measure state $|\psi\rangle$ with M, we get value m_i with probability $\|P_i|\psi\rangle\|^2 = \langle\psi|P_i|\psi\rangle$ and the resulting state is $\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$.

Notice that

- a projector P_i is a positive semi-definite matrices,
- the condition $\sum_i P_i = I$ and the fact that P_i's are projectors, imply $P_iP_j = 0$ for all pairs $\{i, j\}$.

In other words, P_i are orthogonal projectors whose corresponding subspaces span the entire space.

Exercise 12. Show that $I \succeq P_i \succeq 0$. Where $A \succeq B$ means $A - B$ is positive semidefinite matrix.

This definition of projective measurement and the subsequent definition of other kind of measurements is taken as a postulate. We will not worry about, why are measurements defined this way? Though, note that it agrees with the intuition we had about measurement (projecting into subspaces).

When we say that the state is measured in the basis $\{v_1, v_2, \cdots, v_n\}$; it means the projections are,

$$\{P_1 = |v_1\rangle\langle v_1|, P_2 = |v_2\rangle\langle v_2|, \cdots, P_k = |v_k\rangle\langle v_k|\}.$$

In this case, it is easy to come up with the average value of the measurement. You will show in the assignment, the average value of measurement M on $|\psi\rangle$ is $\langle\psi|M|\psi\rangle$.

As a special case, suppose there are two registers, and we measure only the first one with projectors $P_1, P_2, \cdots, P_k$.

Exercise 13. Given that the state could be entangled, what is the action on the combined state?

We take cue from the fourth postulate, the entire system (of two qubits) is measured with respect to projectors $P_1 \otimes I, P_2 \otimes I, \cdots, P_k \otimes I$.

A simpler way to execute this is to project the state onto the required subspace and normalize it. To take an example, suppose we measure the second qubit in the two qubit system, $\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$.

We will measure 0 (corresponding to P_0) with probability $|\alpha_1|^2 + |\alpha_3|^2$ (in the subspace spanned by $|00\rangle, |10\rangle$). The state will be projected to $\alpha_1|00\rangle + \alpha_3|10\rangle$; the final state (normalized) will be $\frac{1}{|\alpha_1|^2+|\alpha_3|^2}(\alpha_1|00\rangle + \alpha_3|10\rangle)$.

Exercise 14. Write the probability of measuring 1 in the second register and the final state after that.

Third postulate: As we hinted above, a more general class of measurements can be defined. This gives us our third postulate.

Postulate 3: A state $|\psi\rangle$ can be measured with measurement operators $\{M_1, M_2, \cdots, M_k\}$. The linear operators M_i's should satisfy $\sum_i M_i^* M_i = I$. The probability of obtaining outcome i is $p(i) := \langle\psi|M_i^* M_i|\psi\rangle$, and the state after measurement is $\frac{M_i|\psi\rangle}{\sqrt{p(i)}}$.

Exercise 15. Prove that the condition $\sum_i M_i^* M_i = I$ is equivalent to the fact that measurement probabilities sum up to 1.

Exercise 16. Show that projective measurements are a special case of measurements defined in the postulate.

Exercise 17. Find a measurement that is not projective.

Notice that the individual measurement operators are not unitary. We made the resulting vector a unit vector by dividing it with its norm.

It turns out that given *ancilla* (additional quantum system) we can simulate any general measurement operator using unitary operators and projective measurements, Section 2.3.

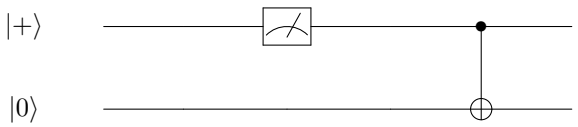
2.1 Principle of deferred measurement

We have seen two *kinds* of transformations on the state of a quantum system, operations and measurements. In a general quantum algorithm/circuit, these two can potentially be interleaved and applied many times. Thankfully, *the principle of deferred measurements* allows us to change this order so as to suit our needs.

To be precise, it says that all measurements can be deferred to the end using ancilla qubits. In simple terms (and to some degree incorrect), whether we mesure the qubits in the end or at the intermediate stage in a circuit, the outcome is same. Let us start with this simple (and slightly incorrect) understanding, we will modify it going forward.

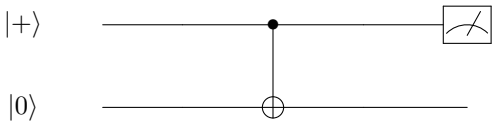
It allows us to analyse our quantum circuit in terms of one single quantum state [1]. For an actual quantum circuit design, moving measurements before could finish the computation using less number of quantum bits. We will see how this principle allows us to perform *quantum teleportation* later.

I hope you are convinced about the importance of this principle, so let us explore. Consider the following quantum circuit.



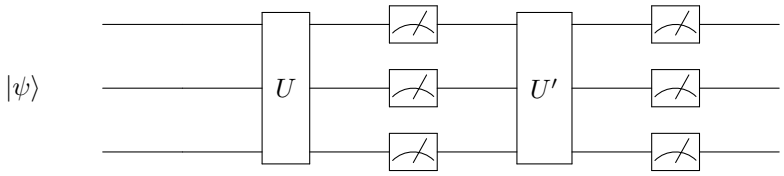
[1] There is a way to capture probabilistic answers in a quantum state (using density matrix formulation), but we will not introduce the formulation here.

What is the state of the second qubit. After measurement, the first state will be in $|0\rangle$ and $|1\rangle$ with equal probability. So, the second state (after application of CNOT) will be in $|0\rangle$ and $|1\rangle$ state with probability $1/2$. What happens if we interchange the order of measurement and CNOT?

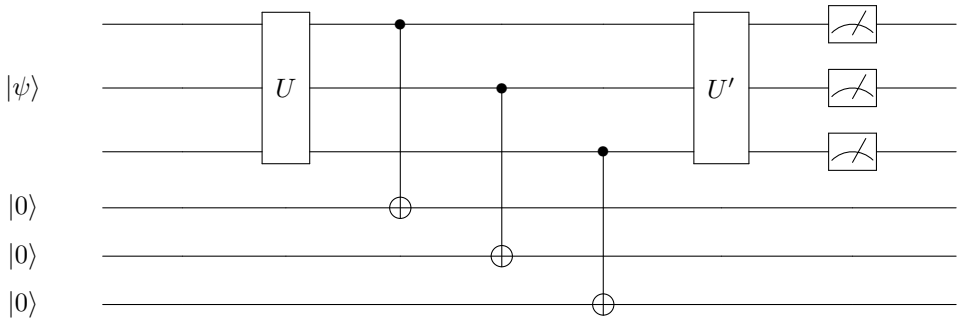


Convince yourself that the second state is in either of the basis states with equal probability (same as the previous circuit). This property remains true for general quantum circuits. The measurements can be moved to the end without affecting the outcome. Actually, it is important that we use ancilla qubit to store the measurement outcome, otherwise we might not get the same outcome (Exercise 28).

So the correct statement would be, using ancilla qubits we can postpone measurements to the end of the circuit. The notes from Melkebeek [1, Lecture 4] give a general strategy for moving measurement to the end. More specifically, the following two circuits have equivalent outcomes.



We use CNOT's on ancilla's to remove measurements.



For a proof and more details, please refer to excellent notes from Dieter van Melkebeek [1, Lecture 4]. We notice two points. First, we need ancilla qubits to make equivalent circuit with measurements at the end. Second, we need ancilla qubits and CNOT because the measurement outcome is kept in the ancilla qubits. For example, suppose after U the state of the circuit is $\sum_{z\in\{0,1\}^m} \alpha_z|z\rangle$. Here $|z\rangle$ are the basis states and α_z is their amplitude. You can show that the state after CNOT will be $\sum_{z\in\{0,1\}^m} \alpha_z|z\rangle|z\rangle$. In other words, the second register will remember the measurement output.

2.2 POVM

For the complete specification of measurement postulate, we defined the probability of getting an outcome and the state of the system after the measurement. Sometimes, we are not interested in the state after the measurement, for instance, measurement is the last step in the algorithm. In that case there is an easier description of measurements.

Notice that the probability in the third postulate only depends upon matrices $M_i^* M_i$ and not the individual matrices M_i. So, we only need to specify $E_i := M_i^* M_i$ to get the probabilities of outcomes. These matrices E_i's are called the *POVM elements* for the measurement.

Note 5. POVM is an abbreviation and stands for *positive-operator valued measure.*

Now, we can understand the third postulate in terms of POVM's without worrying about the individual matrices M_i's. Suppose, we are given $\{E_1, E_2, \cdots, E_k\}$, such that, $\sum_i E_i = I$ and $E_i \succeq 0$ for all i. Then, the POVM measurement $\{E_i\}_i$ on $|\psi\rangle$ gives outcome i with probability $\langle\psi|E_i|\psi\rangle$.

Exercise 18. What are the POVM elements for the projective measurement.

Exercise 19. Show that the state $|\psi\rangle$ and the state $e^{i\theta}|\psi\rangle$ have the same measurement statistics for any measurement.

Such states, differing from each other by an extra $e^{i\theta}$ factor, are said to have a global phase difference and are identical for quantum computing purposes. This is because no measurement can distinguish between these two states. You should not get confused by this and the pair of states $\alpha_0|0\rangle+\alpha_1|1\rangle$ and $\alpha_0|0\rangle+e^{i\theta}\alpha_1|1\rangle$, they differ by a local phase and can be distinguished. For example, $|+\rangle := |0\rangle + |1\rangle$ and $|-\rangle := |0\rangle - |1\rangle$ have a local phase, but they are definitely not identical. You will see that we will use these states, and their difference, are used a lot in quantum computing.

2.3 Extra reading: General measurements using projective measurements

We can use fourth postulate to simulate generalized measurement using projective measurements and unitary operators. Suppose, we would like to perform measurements $\{M_i : 1 \leq i \leq k\}$ on a Hilbert space H. Consider a state space M with basis $\{|1\rangle, |2\rangle, \cdots, |k\rangle\}$.

Note 6. Such extra spaces are needed in quantum computation because it is reversible and are known as *ancilla* systems.

Exercise 20. Read about ancilla bit in quantum computation.

Pick a fixed state $|0\rangle$ in the state space M and define a unitary U on the space $H \otimes M$,

$$U|\psi\rangle|0\rangle = \sum_i M_i|\psi\rangle|i\rangle.$$

Exercise 21. Show that U preserves the norm between states of the form $|\psi\rangle|0\rangle$.

Exercise 22. Show that U can be extended to a unitary operator on the entire space.

Then, the projective measurements can be defined as $P_i := I_H \otimes |i\rangle\langle i|$.

Exercise 23. Show that the probability of obtaining i using the general measurement on $|\psi\rangle$ is same as the probability of getting i when $U|\psi\rangle|0\rangle$ is measured with $\{P_i\}$.

Hence the probability $p(i)$ of obtaining the outcome i matches with the generalized measurement. The combined state of the system using the measurement postulate is,

$$\frac{P_i U|\psi\rangle|0\rangle}{\sqrt{p(i)}} = \frac{M_i|\psi\rangle|i\rangle}{\sqrt{p(i)}}.$$

Suppose, the outcome from the measurement is i. Then, the state of system M is $|i\rangle$ and state of system H is $\frac{M_i|\psi\rangle}{\sqrt{p(i)}}$ after the measurement. Notice that the state and the probability of the outcome of the projective measurement matches with the generalized measurement. In other words, we are able to a simulate general measurement using ancilla system, unitary operator and projective measurement.

3 Assignment

Exercise 24. Show that a matrix M is positive semi-definite if it is the Gram matrix of vectors $|u_1\rangle, \cdots, |u_n\rangle$. That is,

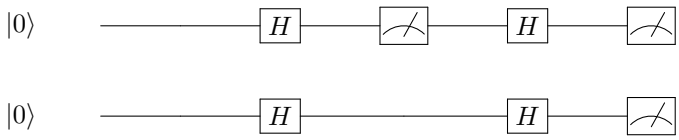
$$M_{ij} = \langle u_i | u_j \rangle.$$

Exercise 25. Show that the property of being positive semidefinite, Hermitian and unitary is preserved under a unitary basis transformation.

Exercise 26. Show that a normal matrix is a projector if and only if all its eigenvalues belong to the set $\{0, 1\}$.

Exercise 27. Given an orthonormal basis $\{|x_1\rangle, |x_2\rangle, \cdots, |x_n\rangle\}$ of the space $\mathbb{C}^n$, show that $\sum_i |x_i\rangle\langle x_i| = I$.

Exercise 28. Show that the output of these two wires are different.



Exercise 29. Let $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ be a quantum state. Find a quantum state orthogonal to $|\psi\rangle$. Write the basis change operator from standard basis to these new states.

References

1. D. Melkebeek. Quantum algorithms, 2023. `https://pages.cs.wisc.edu/~dieter/Courses/2023s-CS880/past-notes.html`.